IN THE CLAIMS

Amended claims follow. Insertions are underlined, while deletions are struck out. The status of each claim is included prior to each heading.

1. (Currently Amended) A computerized method for automatically configuring a firewall operating within an individual computer comprising:

determining a zone for a network address dynamically assigned to a network adapter in the individual computer; and

associating a security policy for the zone with the network adapter, the security policy specifying the firewall configuration to protect the individual computer;

wherein the security policy is defined by a policy file which includes a policy file data structure stored as an XML (extensible markup language) document;

wherein a security policy section of the policy file data structure includes an entry for each security policy that is identified by a policy identifier field and is associated with a network protocol that is identified by a protocol identifier field;

wherein the security policy section specifies filters for at least a portion of ports and services defined by the network protocol, and each port and service associated with the security policy is identified by an element identifier field, a field containing filter settings, and a log indicator field;

wherein at least one security policy is included for a TCP/IP network and includes a PPTP (point-to-point tunneling protocol), a RIP (routing information protocol), a DHCP (dynamic host configuration protocol), an ARP (address resolution protocol), an Ident (identification protocol), ICMP (internet control message protocol) and VPN (virtual private networking) ports, and a NetBIOS (network basic input/output system) service;

wherein a default setting for a high security policy on the TCP/IP network disallows incoming network traffic through the PPTP and ICMP ports, allows incoming network traffic through the RIP, DHCP, ARP and VPN ports, disallows access through the NetBIOS service to shared resources on the individual computer, and disallows the individual computer from using shared resources of other computers on the TCP/IP network, where incoming network traffic that attempts to access the individual computer using PPTP and NetBIOS is logged;

wherein a zone section of the policy file data structure includes an entry for each defined address zone and includes an identifier field, an address parameters field that defines the zone, and an identifier field for the security policy assigned to the zone;

wherein a default zone is defined by addresses that are outside another zone;

wherein the determining and associating is performed when the network address for the network adapter changes;

wherein the security policy associated with the network protocol is specific to the network protocol.

2. (Original) The computerized method of claim 1 further comprising:

determining the network address assigned to the network adapter.

3. (Original) The computerized method of claim 1, wherein the zone is defined by a set of network addresses.

4. (Original) The computerized method of claim 3, wherein the set of network addresses comprises at least one address within the zone.

5. (Previously Presented) The computerized method of claim 3, wherein the set of network addresses comprises at least one address outside the zone.

6. (Original) The computerized method of claim 1 further comprising:

assigning the security policy to the zone.

7. (Previously Presented) The computerized method of claim 1 further comprising:

retrieving the policy file that contains definitions for the zone and the security policy and specifies that the security policy is assigned to the zone.

8. (Original) The computerized method of claim 7 further comprising:

creating the policy file from data input by a user.

9. (Original) The computerized method of claim 7 further comprising:

creating the policy file from data input by an administrator.

10. (Previously Presented) The computerized method of claim 7 further comprising:

receiving data from a predetermined location on the network through the network adapter; and

creating the policy file from the data.

11. (Currently Amended) A computer-readable medium having computer-executable instructions to automatically configure a firewall operating within an individual computer comprising:

determining a zone for a network address assigned dynamically to a network adapter in the individual computer; and

associating a security policy for the zone with the network adapter, the security policy specifying the firewall configuration to protect the individual computer;

wherein the security policy is defined by a policy file which includes a policy file data structure stored as an XML (extensible markup language) document;

wherein a security policy section of the policy file data structure includes an entry for each security policy that is identified by a policy identifier field and is associated with a network protocol that is identified by a protocol identifier field;

wherein the security policy section specifies filters for at least a portion of ports and services defined by the network protocol, and each port and service associated with the security policy is identified by an element identifier field, a field containing filter settings, and a log indicator field;

wherein at least one security policy is included for a TCP/IP network and includes a PPTP (point-to-point tunneling protocol), a RIP (routing information protocol), a DHCP (dynamic host configuration protocol), an ARP (address resolution protocol), an Ident (identification protocol), ICMP (internet control message protocol) and VPN (virtual private networking) ports, and a NetBIOS (network basic input/output system) service;

wherein a default setting for a high security policy on the TCP/IP network disallows incoming network traffic through the PPTP and ICMP ports, allows incoming network traffic

through the RIP, DHCP, ARP and VPN ports, disallows access through the NetBIOS service to shared resources on the individual computer, and disallows the individual computer from using shared resources of other computers on the TCP/IP network, where incoming network traffic that attempts to access the individual computer using PPTP and NetBIOS is logged;

wherein a zone section of the policy file data structure includes an entry for each defined address zone and includes an identifier field, an address parameters field that defines the zone, and an identifier field for the security policy assigned to the zone;

wherein a default zone is defined by addresses that are outside another zone;

wherein the determining and associating is performed when the network address for the network adapter changes;

wherein the security policy associated with the network protocol is specific to the network protocol.

12. (Original) The computer-readable medium of claim 11 having further computer-readable instructions comprising:

determining the network address assigned to the network adapter.

13. (Original) The computer-readable medium of claim 11 having further computer-readable instructions comprising:

assigning the security policy to the zone.

14. (Previously Presented) The computer-readable medium of claim 11 having further computer-readable instructions comprising:

retrieving the policy file that contains definitions for the zone and the security policy and specifies that the security policy is assigned to the zone.

15. (Original) The computer-readable medium of claim 14 having further computer-readable instructions comprising:

creating the policy file from data input by a user.

16. (Original) The computer-readable medium of claim 14 having further computer-readable instructions comprising:

creating the policy file from data input by an administrator.

17. (Previously Presented) The computer-readable medium of claim 14 having further computer-readable instructions comprising:

receiving data from a predetermined location on the network through the network adapter; and

creating the policy file from the data.

18. (Original) The computer-readable medium of claim 11 having further computer-readable instructions comprising:

defining the zone based on a set of network addresses.

19. (Original) The computer-readable medium of claim 18 having further computer-readable instructions comprising:

including at least one address within the zone in the set of network addresses.

20. (Original) The computer-readable medium of claim 18 having further computer-readable instructions comprising:

including at least one address outside the zone in the set of network addresses.

21. (Currently Amended) A computerized system comprising:

a processing unit;

a memory coupled to the processing unit through a bus;

a network adapter coupled to the processing unit through the bus and further operable for coupling to a network;

a firewall process executed from the memory by the processing unit to protect the computerized system when the network adapter is coupled to a network by causing the processing unit to filter data addressed to the network adapter according to a security policy; and

a firewall configuration process executed from the memory by the processing unit to cause the processing unit to determine a zone for a network address dynamically assigned to the network adapter and to associate a firewall security policy for the zone with the network adapter;

wherein the security policy is defined by a policy file which includes a policy file data structure stored as an XML (extensible markup language) document;

wherein a security policy section of the policy file data structure includes an entry for each security policy that is identified by a policy identifier field and is associated with a network protocol that is identified by a protocol identifier field;

wherein the security policy section specifies filters for at least a portion of ports and services defined by the network protocol, and each port and service associated with the security policy is identified by an element identifier field, a field containing filter settings, and a log indicator field;

wherein at least one security policy is included for a TCP/IP network and includes a PPTP (point-to-point tunneling protocol), a RIP (routing information protocol), a DHCP (dynamic host configuration protocol), an ARP (address resolution protocol), an Ident (identification protocol), ICMP (internet control message protocol) and VPN (virtual private networking) ports, and a NetBIOS (network basic input/output system) service;

wherein a default setting for a high security policy on the TCP/IP network disallows incoming network traffic through the PPTP and ICMP ports, allows incoming network traffic through the RIP, DHCP, ARP and VPN ports, disallows access through the NetBIOS service to shared resources on the individual computer, and disallows the individual computer from using shared resources of other computers on the TCP/IP network, where incoming network traffic that attempts to access the individual computer using PPTP and NetBIOS is logged;

wherein a zone section of the policy file data structure includes an entry for each defined address zone and includes an identifier field, an address parameters field that defines the zone, and an identifier field for the security policy assigned to the zone;

wherein a default zone is defined by addresses that are outside another zone;

wherein the firewall configuration process is executed by the processing unit when the network address for the network adapter changes;

wherein the security policy associated with the network protocol is specific to the network protocol.

22. (Cancelled)

23. (Cancelled)

24. (Original) The computerized system of claim 21 wherein the firewall configuration process further causes the processing unit to determine the network address of the network adapter.

25. (Previously Presented) The computerized system of claim 21 wherein the firewall configuration process further causes the processing unit to define the zone based on a set of network addresses.

26. (Original) The computerized system of claim 25, wherein the set of network addresses comprises at least one address within the zone.

27. (Original) The computerized system of claim 25, wherein the set of network addresses comprises at least one address outside the zone.

28. (Previously Presented) The computerized system of claim 21, wherein the firewall configuration process further causes the processing unit to assign the security policy to the zone.

29. (Previously Presented) The computerized system of claim 21, wherein the firewall configuration process further causes the processing unit to retrieve the policy file that contains definitions for the zone and the security policy and specifies that the security policy is assigned to the zone.

30. (Previously Presented) The computerized system of claim 29, wherein the firewall configuration process further causes the processing unit to receive data from a user and to create the policy file from the data.

31. (Previously Presented) The computerized system of claim 29, wherein the firewall configuration process further causes the processing unit to receive data from an administrator and to create the policy file from the data.

32. (Previously Presented) The computerized system of claim 29, wherein the firewall configuration process further causes the processing unit to receive data from a predetermined location on the network through the network adapter and to create the policy file from the data.

33-40. (Cancelled)

41. (New) The computerized method of claim 1, wherein the network address dynamically assigned to the network adapter is determined by mapping an adapter registry identifier to an associated network address stored in an operating system registry.

42. (New) The computerized method of claim 1, wherein the network address dynamically assigned to the network adapter is determined by monitoring network traffic at the network adapter and examining a predefined limited amount of the network traffic to determine the network address.

43. (New) The computerized method of claim 1, wherein the network address dynamically assigned to the network adapter is determined by receiving a network address from a network adapter device driver when the network adapter connects to the TCP/IP network.